DOI: http://dx.doi.org/10.26483/ijarcs.v11i5.6651

Volume 11, No. 5, September-October 2020

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

PRIVACY-PRESERVING DATA AGGREGATION IN INTERNET OF THINGS (IOT): AN OVERVIEW

Manas Ranjan Mohapatra
Research Scholar
Department of Computer Application
SSSUTMS, Sehore
M.P., India

Dr. Jitendra Sheetlani
Associate Professor
Department of Computer Application
SSSUTMS, Sehore
M.P., India

Dr. Rasmi Ranjan Patra
Assistant Professor
Dept. of CSA
CPGS, OUAT
Bhubaneswar, India

Abstract: IoT devices enhance efficiency, accuracy and economic advantages along with less involvement of human resources, thus our different daily applications have become more flexible and convenient. But, in IoT we have many security and privacy challenges emerging on regular basis. Earlier this issue has been addressed by introduction of many approaches for achieving privacy-preserving in data aggregation process. In this aspect this paper presents an outline of IoT-oriented approach for achieving privacy preservation together with minimizing communication overhead. This paper reviews the latest Privacy Preserving Data Aggregation (PPDA) techniques along with their comparative analysis. Latest techniques are investigated here to give a detail analysis of the each and every step of these techniques. In addition, every mathematical operation used in several PPDA schemes is analyzed here. Also current study will be advantageous to researchers in designing solutions in terms of energy efficiency and computational feasibility for ensuring user privacy in different IoT application.

Keywords: Privacy, Internet of Things, Computing, Network, Sensor, Security, Data Aggregation, Communication Overhead.

I. INTRODUCTION

In modern age of computing, Internet of Things has been an important technology. IoT is an interaction of internet connected smart entities. IoT is viewed as a system comprising of objects, related computational devices, people/animals, mechanical/digital machines, having unique identifiers along with ability to transmit data over a network without human-to-device /human-to-human or interaction. Data transmission over wireless networks possibly have private/secret data, thereafter this type of system involves security problems like planned crimes, cyber-attacks and private privacy. In order to accomplish these issues, it must have certain features such as Privacy-Preserving and data aggregation [1].

In society personal privacy is always considered as a major aspect. Privacy is one of the basic issue to interlink WSNs in IoT with civilian applications, where unusual person may try for determining detail information in more by monitoring their neighbors communications. Data aggregation is a method introduced in IoT for significant reduction of sensor node's energy usage along with communication overhead in data collection development. But, in data aggregation privacy preservation is a major challenge, where aggregators required performing few aggregation operations on received sensing data. Sensor node and sensor network life can be increased with efficient data aggregation approach, since this one reduces communication overhead along with each node's computation in network.

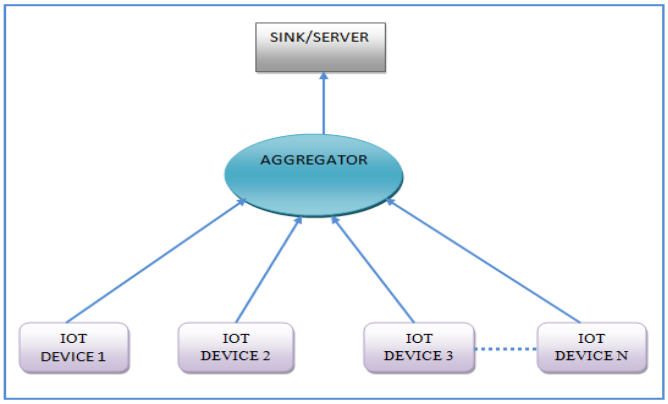

Figure 1. Data aggregation in IoT

Here, an efficient privacy-preserving data aggregation method is discussed for IoT. Additionally, an analysis is presented for privacy-preserving data aggregation in IoT.

Latest techniques are reviewed here too along with security and privacy issues are also analyzed. Also know about, Data Aggregator that performs aggregation of received data while unaware of individual's actual data. So far our knowledge is concerned; it is the recent most discussion on PPDA solutions. We have organized the paper as; section 2 discuss PPDA methods in resource-constrained sensor nodes, section 3 gives

an analysis of these methods and at last, section 4 concludes our discussion.

II. PRIVACY-PRESERVING DATA AGGREGATION METHODS

Most IoT applications need certified security and privacy levels. An important concern in WSNs is to provide effective data aggregation by preserving data privacy. Many privacy-preserving data aggregation approaches we have so far for smart grid and WSN. Few PPDA methods are reviewed here and their operations are compared. These methods are briefly summarized as follows.

Bista et al. [2] designed a method for privacy preservation of WSN data from security threats. Present approaches like "cluster-based private data aggregation (CPDA)" and "Slice-Mix-AggRegaTe (SMART)" [3] possess higher cost of communication. But these are efficient proposed method and gives better performance from both energy dissipation and communication overhead aspect.

Li et al. [4] proposed a very good sum aggregation protocol that uses an additively homomorphic encryption, and using this protocol they additionally constructed a high-efficient Min computation protocol. In addition to smart protocol design and good efficiency, Li et al.'s protocols uses a fine elegant key system by which these protocols defend collusion attack thus will be potential to efficiently handle users' dynamic joining and leaving.

Yip et al. [5] used Incremental Hashing Function for introducing a "Privacy-preserving and Cheat-Resilient (PPCR)" electric consumption and reporting for Smart Grid (SG). IHF requires reduced computation and storage power thus appropriate for resource-constrained smart meter. This system performs hashing and data aggregation on smart meter. It is a highly secure as well as privacy based system. It does not give result in case of data eavesdropping at device layer.

Kumar and Madria [6] designed a novel energy efficient algorithm to preserve data privacy and integrity in data aggregation process. It is formulated upon Recursive Secret Sharing (RSS) and shares data δ used to store k-2 additional pieces of information. A node having minimum k shares can simply rebuild all k-1 pieces of secret information. It provides a construction that prevents a node with all shares, from rebuilding and fetching secret data. This is very efficient algorithm considering processing time, energy utilization, memory use and bandwidth utilization aspects. This algorithm does not discuss method to support variables in sensor nodes.

Othman et al. [7] designed a method where data privacy is ensured through aggregation thus improves data transmission efficiency. This method is founded on homomorphic symmetric encryption and achieves data integrity by use of homomorphic signature. An energy efficient data aggregation method is designed by Othman et al. [8] for data privacy and integrity which is secure against node compromise attack. It uses "Elliptic Curve Okamoto-Uchiyama (EC-OU)" to ensure data privacy together with "Elliptic Curve Digital Signature Algorithm (ECDSA)" to maintain data integrity in data aggregation process of WSN.

We basically summarize state-of-art of PPDA schemes. Current privacy preserving data aggregation scheme gives privacy protection as user's private data or disclosing intermediate information. We discussed different efficient practical data aggregation methods where collected data are confused for preserving users' privacy.

III. NEEDS OF PRIVATE DATA AGGREGATION

The main design objective here is to give an analysis of privacy-preserving data aggregation structure, which is strong against eavesdropping, also have the potential of detecting data pollution and node crashes. Data privacy protection in many IoT applications is a main issue. Key characteristics of a private data aggregation approach can be summarized as the following criterions [3, 9]:

1) Privacy: It is one of the key problems for applying IoT networks, where every node data is to be known to that node only. Privacy is measured as a major aspect of maintaining data without data loss. Moreover, private data aggregation methods must possess ability for managing certain attacks partially and collision between compromised nodes. Whenever a sensor network subject to different malicious attack, we may have possibility that few nodes may collide for retrieving other node(s) private data. Developing better privacy-preserving data aggregation systems is vital for ensuring adequate and strong data privacy against these attacks.

2) Energy Efficiency: Resource and power utilization feature of IoT Sensor determines its lifetime. The data aggregation reduces message numbers communicated in a sensor network; thereby decrease resource and energy utilization. Use of in-network processing causes data aggregation to achieve bandwidth efficiency. We cannot ignore the additional overhead which is introduced in private data aggregation systems for protecting privacy. An appropriate efficient system should keep that additional payload size, computational cost, communication overhead and memory comparatively small.

3) Data Accuracy: Possibility of data loss may encounter due to wireless link during communication or node failure thus affecting result accuracy. So there is a need of an accurate sensor data aggregation having constraint that accurate value of any separate sensor should not know to other sensors. For performance evaluation of private data aggregation schemes, accuracy should be a measure.

4) Fault Tolerance: Malfunctioning of sensor nodes are due to unauthorized attack, lack of energy and hardware failure. IoT network should be powerful and strong against this issue of sensor nodes and preservation of network functionality should be there. To make up failure nodes here must be addition of new nodes to network. Node accumulation should be allowed in data aggregation to preserve network functionality in a best system.

5) Flexibility: IoT network must be flexible. Additionally, system must be convenient for inclusion of new node in residential area.

6) Data Integrity: Results of data aggregation may be utilized for developing critical conclusions, need of a base station for

attesting integrity of aggregated result prior to acceptance. So, it is preferred that data aggregation method has integrity check ability.

IV. COMPARATIVE ANALYSIS

In this part, we give the performance analysis of existing Privacy preserving data aggregation algorithms for IoT. Basic performance parameters include Communication Overhead, Computation Cost, Privacy level and Privacy against aggregator IoT sensor node [10].

Computational Cost (CC): It is the evaluation of algorithm in terms of complexity of mathematical iterations used.

Communication Overhead: It is the total numbers of packets to be transferred or transmitted from one node to another.

Privacy preservation Level and Privacy against aggregator: Ensure data privacy against eavesdropping.

The comparative analysis of different techniques can be summarized as in the following table.

Table 1. Comparative analysis of PPDA Techniques for IoT

Techniques	Privacy preservation efficiency	Communication overhead	Aggregation accuracy	Computational overhead	Privacy against aggregator
CPDA	Excellent	Fair	Good	Fair	Yes
SMART	Excellent	Large	Good	Small	Yes
PPCR	High	Very Small	-	Medium	No
PIP	Medium	Medium	-	Medium	Yes
SPDA	-	Light-weighted	Very High	-	Yes
EC-OU & ECDSA	High	Small	-	Very High	Yes

The above table provides a comparative analysis of these state-of-art techniques based on different performance measuring parameters. These parameters forms preferred features of any privacy algorithm in Internet of Things.

V. CONCLUSION AND FUTURE WORK

PPDA is a basic approach to save communication bandwidth for private data collection in WSNs. In this discussion, we analyzed privacy preserving data aggregation system in IoT as well as identified various issues in designing privacy preserving data aggregation. This in-depth analysis will produce novel research strategies in expanding existing systems and implementing advanced secure and privacy preserving data aggregation system for IoT. Existing privacy-preserving data aggregation protocols have used different system like shuffling, privacy homomorphism and perturbation to achieve data privacy. Each type of the above systems has some advantages and disadvantages.

In this review article, we also analyzed existing PPDA in IoT sensor nodes and provided comparison of existing methods with respect to many performance parameters. This analysis will assist new researchers for realizing PPDA method and can be helpful to propose more efficient privacy-preserving techniques.

Future work involves extension to implement an Efficient and secure privacy-preserving data aggregation approach for IoT along with enhancing efficiency of communication overhead and power dissipation. Another aim of this proposed research is this approach can resist against the false data injection from the external attacks.

VI. REFERENCES

[1] Atzori L, Iera A, Morabito G, “The Internet of Things: a survey”, Compute Netw 2010; 54:2787-805.

[2] Bista R, Jo K, Chang J, “A new approach to secure aggregation of private data in wireless sensor networks”, in IEEE international conference on dependable, autonomic and secure computing; 2009. p. 394-9.

[3] He W, Liu X, Nguyen H, Nahrstedt K, Abdelzaher T, “PDA: privacy preserving data aggregation in wireless sensor networks”, in Proceedings of the INFOCOM; May 2007. p. 2045-53.

[4] Q. Li and G. Cao, “Providing efficient privacy-aware incentives for mobile sensing”, in Proc. IEEE 34th Int. Conf. Distrib. Comput. Syst. (ICDCS), Madrid, Spain, Jun./Jul. 2014, pp. 208–217.

[5] Yip S, Wong K, Phan R, Tan S, Ku I, Hew W, “A privacy-preserving and cheat-resilient electricity consumption reporting scheme for smart grids”, In: International conference on computer, information and telecommunication systems, CITS; 2014. p. 0-4.

[6] Kumar V, Madria S, “PIP: privacy and integrity preserving data aggregation in wireless sensor networks”, in IEEE 32nd international symposium on reliable distributed systems (SRDS); 2013. p. 10-9.

[7] Othman S., Bahattab A., Trad A, “Confidentiality and integrity for data aggregation in WSN using homomorphic encryption”, Wireless Pers Commun, 80 (2) (2014), pp. 867-889.

[8] Othman S, Alzaid H, Trad A, “An efficient secure data aggregation scheme for wireless sensor networks”, in IEEE international conference on information, intelligence, systems and applications (IISA); 2013.

[9] I. Memon, (2012). “An Analysis of Privacy Preserving Data Aggregation Protocols for WSNs”, Network and Parallel Computing, 7513: pp.119- 128.

[10] Inayat Ali et al., “Privacy-Presereving data aggregation in Resource-Constrained Sensor Nodes in Internet of Things: A Review”, DOI: 10.1016/j.fcij.2017.11.004.